

## **A CASE STUDY OF EVALUATING SECURITY IN AN OPEN SYSTEMS ENVIRONMENT**

### **Authors:**

Daniel L. Tobat , TASC, formerly The Analytical Sciences Corporation,  
12100 Sunset Hills Road, Reston VA 22090      Tel: 703.834.5000  
Fax: 703.318.7900    E-mail: dltobat@tasc.com    Web: www.tasc.com

Errol S. Weiss, Technical Director, Science Applications International Corporation's  
Center for Information Protection, 8301 Greensboro Drive, McLean, VA 22102  
Tel: 703.556.7366    Fax: 703.448.7360    E-mail: errol@cip.saic.com

### **Abstract**

The goal of this paper is to describe a case study of a computer security evaluation effort conducted on a system known as the Office Automation Network (OAN). The OAN is representative of many of today's networked systems by being a heterogeneous mix of system components connected to open systems such as the Internet. The OAN differs from typical systems in that security was a design and implementation objective, and that it was subjected to an extensive six month evaluation effort by an experienced vulnerability testing team. The vulnerability testing yielded some surprising results which demonstrated that it is possible in today's environment to have an Automated Information System (AIS) connected to open systems such as the Internet and still have an effective security posture.

### **Introduction**

The large scale networking of Automated Information Systems (AIS) on a worldwide basis has implications for the information systems security field which are only now becoming widely recognized. The ability of current information technology to network and interconnect systems has in most cases far outpaced the ability to protect these networks. In the interest of interoperability, widespread sharing of information and doing more work with a smaller, more technically agile workforce, the push is on to increasingly network systems and to connect these AIS to globally interconnected "network of networks" such as the Internet. The increased efficiency of AIS networking has generally come at the price of increased vulnerability of systems and information to attack. An AIS connected to open systems environments such as the Internet can be accessed worldwide thus exposing systems to a wide range of potential security threats. In the networked environment of operational systems, not only is it more of a challenge to protect systems, it also becomes increasingly difficult to determine the security posture of a networked system. As technology increasingly pushes open systems environments, and as computer and communication technologies continue to converge, it becomes difficult for even system administrators and technical personnel to know the full extent of individual system boundaries and capabilities. This technological convergence often introduces new vulnerabilities into the overall information infrastructure which present potential intruders with more opportunities to target a wider range of information.

## System Description

The OAN has its genesis in the early 90's as an effort to consolidate the architecture and technology of various segmented LAN's which had been separately implemented by different offices. From its inception, the OAN design recognized a need to provide two distinct and separate network segments linked by a central backbone: a "low" side offering users open access to the Internet and a "high" side for users with requirements to protect more sensitive information, yet still requiring shared information services with "low" side users. The OAN is a large scale, general purpose office automation environment, based on a Microsoft Windows-NT client-server architecture encompassing over 1,500 workstations, 30 servers and an external gateway on a Fiber Optic Digital Device Interface (FDDI) backbone ring, with thin-net Ethernet distribution to most client workstations. General office automation services such as E-mail, word-processing, spread sheet and database programs are provided to a user population of approximately 2,000. As shown in figure 1, the OAN is divided into a "high side" segment and a "low side" segment which are essentially mirror images of each other. While the fiber optic cable, servers and gateways are physically separated they are connected through a bi-directional E-mail guard. The E-mail guard is hosted on an Intel-based platform running the SCO/CMW trusted operating system. The OAN's Internet connection is hosted by a Digital Equipment Corporation (DEC) VAX 6310 running the VAX/VMS operating system. A separate DEC VAX 6310 hosts the E-mail guard on the high side of the OAN. In addition to the E-mail guard, the Network Monitoring Stations are the only network elements running the UNIX operating system, which consist of Sun SPARC workstations running the Cabletron Spectrum Network Management Tool Suite. A security policy is in place which limits off network access and permits limited E-mail capability to traveling users through the use of temporary accounts on

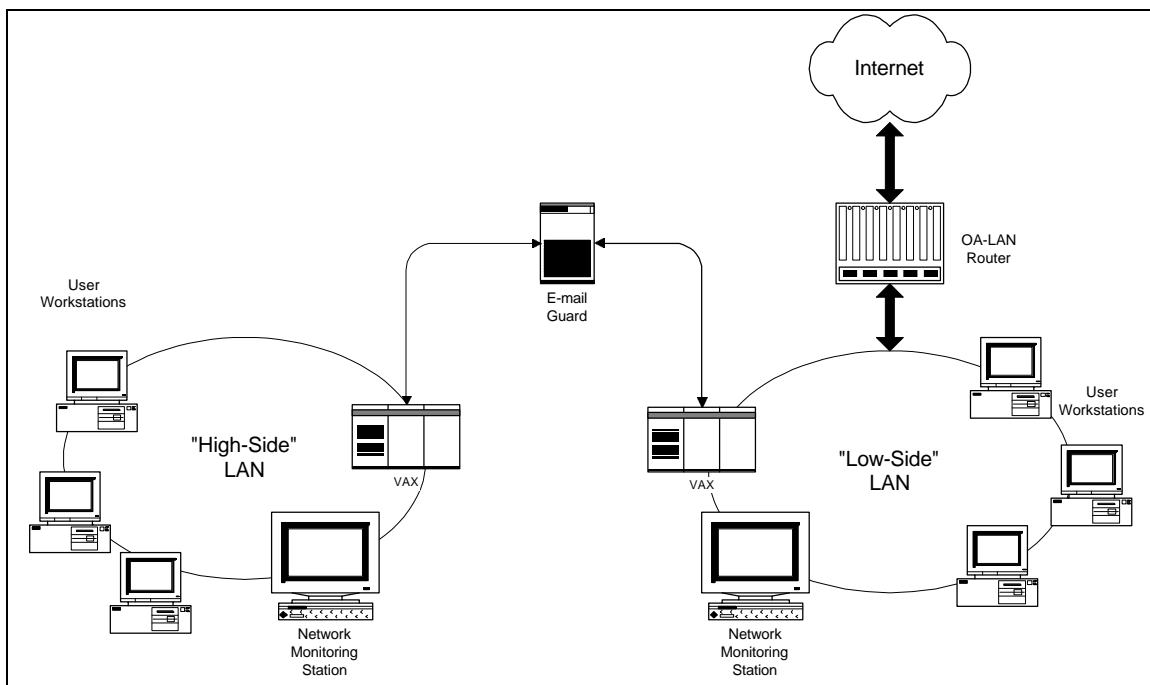


Figure 1. OAN Topology

the DEC/VAX system using static log-in/password procedures. The OAN was undergoing continual evolution during the six month course of this evaluation, such as upgrading the VAX 6310 hosts to DEC Alpha hosts which run both VAX/VMS and Windows. Packet filtering is employed by the OAN's TIMEPLEX Time/LAN 100 routers as a "firewall" technique. While not implementing a commercial offering of a "firewall," the combination of system features does in fact meet the definition of a "packet filtering firewall" according to the definitions developed by the National Institute of Standards and Technology (NIST) [1].

### **Key Component Descriptions:**

This section provides additional detail on some key OAN components.

**Windows-NT:** This is a modular network operating system, which has been rated by the Trusted Products Evaluation Program (TPEP) at a "C2" level of security. The "C2" rating includes the ability of auditing to allow security related events to be recorded and monitored, the implementation of Discretionary Access Controls (DAC) and requiring Identification and Authentication (I&A) through the use of a mandatory log-in process to access the system. OAN servers run Windows-NT Server V3.51, while OAN clients use a mixture of Windows 3.1, Windows for Workgroups 3.1.1 and Windows-95 operating systems.

**E-mail Guard:** This component consists of a bi-directional E-mail guard that passes electronic messages and attachments between the low and high side LAN segments, and consists of a 486DX-50 MHz Intel platform running Santa Cruz Operating Systems (SCO) UNIX as the underlying operating system. The guard uses the "B1" TPEP rated Compartmented Mode Workstation (CMW) software package along with a custom designed user interface. The "B1" rating indicates the ability to support more restrictive security features than the "C2" rating such as the use of Mandatory Access Controls (MAC). The custom software package implements OAN security policies such as while high side users can send E-mail to low side users, they are not allowed to send E-mail to the Internet host. Low side users can send E-mail to high side users as well as out through the Internet. E-mail messages are encapsulated and signed to provide integrity. Prior to being deployed on the operational network, the E-mail guard underwent a security testing profile in a laboratory environment as a risk reduction technique.

### **The Challenge**

While the OA-LAN had been designed and implemented with security as an objective, it had not been the subject of vulnerability testing by outside security experts. The widespread recent publicity associated with the "information warfare" concept, led to the commissioning of a non-trivial vulnerability testing effort to determine the security posture of the OA-LAN. Accordingly, a team of five personnel, with expertise across the range of OA-LAN systems and a combined vulnerability testing experience level of 33 years was put together to evaluate the OA-LAN. Because the OA-LAN was an operational system supporting thousands of users on a daily basis, it was not practical to exhaustively test for every potential vulnerability or to conduct denial of service attacks. While exhaustive vulnerability testing in a lab type environment is possible with development systems, large scale operational systems are usually too expensive to duplicate in a laboratory, and the consequences of many denial of service attacks can be difficult to predict. The principal objective behind this evaluation was to replicate the threat environment faced by the target system and which is summarized below. Any system connected to the Internet is susceptible to both external and internal threats and as such, should be subjected to periodic evaluations to determine its security posture. Performing a computer security evaluation on the OA-LAN was a challenge for several reasons. Traditionally, the majority of systems evaluated by the computer security community are UNIX systems. By contrast, the OA-LAN was a mixture of operating

systems including Windows-NT, VAX/VMS and UNIX. The need to evaluate a broad range of systems led to an extensive survey phase to fully train the team in the various technologies necessary and to set up a small scale mockup in a lab to explore and determine potential avenues of exploitation.

### **The Threat**

For any system connected to the Internet, there is a very real threat from hackers, which will be defined here as a computer based intruder with no legitimate access on a system, and is also the term by which most computer intruders call themselves [2]. The Internet most closely resembles a global information superhighway, which connects over 35 million users through over 9 million hosts, linked by over 240,000 networks in 135 countries worldwide [3]. The Internet and its underlying Transport Control Protocol/Internet Protocol (TCP/IP) architecture were not designed to be secure. The phenomenal success of the Internet, in combination with the presence of unethical users has aggravated deficiencies to the extent that any system connected to the Internet risks inevitable break-in attempts. Several organizations, such as the Defense Information Systems Agency (DISA) Automated Information Systems Security Support Team (ASSIST) which track Internet intrusions on Department of Defense (DoD) systems, indicate at least one new intrusion attempt per day is now reported. In addition, the ASSIST regularly tests DoD sites with Internet connectivity for well known vulnerabilities which appear in Computer Emergency Response Team (CERT) bulletins. As of October 1994, over 88% of 8900 tested systems were easily penetrated, and 96% of the system penetrations went undetected [4]. The overall conclusion is that any system connected to the Internet can expect to be the target of repeated intrusion attempts and that many of these systems lack rudimentary levels of security. The majority of the widely publicized “information warfare” risk has focused on the external threat posed by hackers. Today’s hackers include experienced, technically sophisticated intruders who have even published price lists for their services, and are willing to perform criminal activities for financial gain [5]. Hackers rely on a loosely organized, yet highly competitive computer “underground” for information exchange. Hackers usually begin by gaining admission to “entry level” groups of lower skilled members, and work their way into smaller groups of more sophisticated “elite intruders” by hacking systems and providing results as a proof of their expertise. In addition to the external hacker, all AIS have an internal threat due to the possibility of unscrupulous users, that is an individual with some degree of legitimate access to the system who performs unauthorized actions. Also worthy of note is the “disgruntled postal worker” syndrome, that is an employee who is losing their job as a result of workforce reductions and attempts to “get even” by sabotaging systems on which they have access. Data reported by the National Center for Computer Crime show that upwards of 85% of reported successful intrusion attacks on public networks are conducted or actively assisted by insiders [6]. In order to perform thorough vulnerability testing on an operational system, one must evaluate both the susceptibility of the system to both the external hacker as well as the “close in” unscrupulous insider.

### **Testing Approach**

The key objective of the testing was to replicate the threat environment by performing various internal as well as external tests, in order to determine the security posture of the OAN. To simulate the external threat, the test team would use a series of standardized tools and scripts to mount attacks remotely across the Internet against the target system. A “standard hacker” tool suite would be run remotely against the OAN, and in addition an “intruder test team” was established to perform on-site internal testing. Internal threat testing usually focuses on the possibility of a user

exploiting network functions in an attempt to “break out of the box” and perform unauthorized functions which are normally restricted to system administrators. For this evaluation, the intent was for the intruder test team to replicate a “best shot” effort by an “elite intruder” hacker group operating with the premise of some on-site access in a two phased effort. In the initial phase, the test team would set up covertly on site, and attempt various “close in” technical exploitation methods without the knowledge of system administrators. During the subsequent phase, “social engineering” tactics would be used in an attempt to obtain user account passwords which would then be used in an attempt to subvert the system security policy from within, and finally various audit activities would take place with the knowledge and assistance of system administrators. The clearly expected result of devoting an experienced computer security testing team in an intensive six month long effort, is to achieve a successful system “break in” and demonstrate how the system could be exploited by outside hackers and or unscrupulous insiders. The experience of the team in past vulnerability testing efforts above led to expectation of a successful penetration with the only major question being the degree of difficulty to achieve intrusion, and whether that intrusion would be detected. Due to the many different computer systems present in the OAN, the five person test team underwent an extensive survey phase, obtaining all possible document on security features and vulnerabilities of the target system, received training on the relatively new Windows-NT operating system, and set up limited mock ups in a laboratory setting to explore different avenues of attack.

### **Vulnerability Testing Results**

After an intense five month long preparation period, both internal and external testing was conducted over a one month period. Key testing activities are graphically depicted on figure 2. The results of these testing activities directed against the OAN were surprising. In an environment, where finding computer security vulnerabilities sometimes of an extensive nature is all too typical, the concluding results of this evaluation was that the OAN had an effective security posture. The “standard hacker” tool suites discovered no vulnerabilities while remotely testing the system. During the initial on-site testing phase, the on-site intruder test team was able to surreptitiously tap into the low side of the OAN by splicing in an extra 50 feet of cable to a “thin net” segment. The intruder test team then used five vulnerability testing stations on the added 50 feet of cable to conduct extensive “insider” testing. However, only minor configuration issues were discovered and the system could not be exploited further. Many of the team’s hacking attempts were detected and reported by an OAN auditing team. During the second phase of the on-site testing, software auditing tools and wardialing were used to test for the presence of unauthorized modems, fax boards, and off-network access. A random sample of OAN workstations found a high rate of compliance with the system security policy. The intruder test team also attempted insider attacks against the E-mail guard in an attempt to gain unauthorized access to the high side of the OAN. The team found that the E-mail guard provides an effective barrier against attempts to access the high side. The test team reported that the auditing, monitoring and reporting procedures used on the OAN were excellent. The consensus of the test team was that the OAN had succeeded in achieving an effective security environment that was highly resilient to intrusion attempts. In view of the relatively poor security on many of the systems connected to the Internet, the OAN thus represents a model of how to implement an effective security posture in an open systems environment. This surprising result led to an intensive analysis to determine why the OAN had such an effective posture.

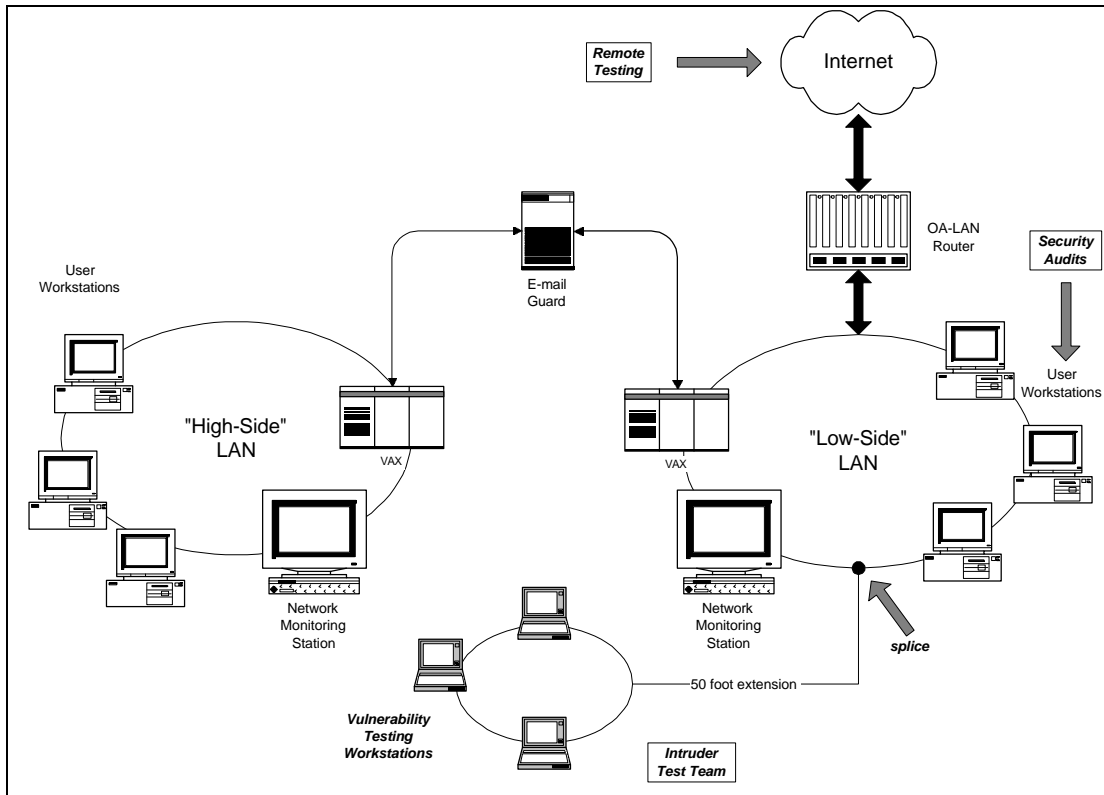


Figure 2. OAN Vulnerability Testing Activities

The unexpected result of finding a system so resilient to intrusion attempts led to an analytical effort to identify the reasons for the OAN's successful posture which led to this atypical outcome. The consensus of this analysis was that the OAN represented a system in which all the key items were present to ensure a strongly postured system including effective security policies, contributing technical factors and the allocation of sufficient resources to effectively secure this system. These specific factors are outlined in detail below.

#### **Effective Security Policies:**

The security policies employed on the OAN reduced risks by strictly limiting the outside connections allowed on the system. Off-network access is carefully controlled. No modem or fax capabilities are permitted and TCP/IP stacks installed on workstations are carefully implemented and frequently monitored to reduce risks. The E-mail accounts for roving users are temporary accounts which only have limited capabilities and are hosted on the DEC VAX processor. These policies are not only carefully designed to limit risks but are also effectively enforced. The on-site audit of a random number of workstations by the intruder test team confirmed that these policies are indeed followed by system users. In addition, the OAN policy of putting system administrators on notice that vulnerability testing could occur at any time without their knowledge is a highly commendable procedure. Note that while the OAN vulnerability testing was a "no notice" event to system administrators and the audit team, it was fully coordinated with site security personnel.

**Contributing Technical Factors:**

Several factors of a technical nature contributed to the OAN's security posture. One major factor was that the OAN was designed with security as an initial objective and was not an "add on" after the system was put together. Experience demonstrates that designing security in from the start is the most effective method to secure a system. The well thought out nature of the OAN's topology contributed to the system's resiliency to intruders. The other contributing factor was the use of the Windows-NT operating system. One of the most effective security features of Windows-NT was the selective use of encryption to protect packets containing log-in and password information, thus effectively limiting the exploitation of the system, even by intruders directly connected to the OAN. The tools used by both hackers and the vulnerability testing community are predominantly based on the UNIX operating system. Because of the widespread use of UNIX, it has been commonly used in multi-user operational environments and has long been the traditional target of computer based intrusions. Since the OAN does not rely on UNIX for the most part, most computer vulnerability tools and methods are ineffective at present. Note this is a transient advantage that will erode over time as the number and lucrativeness of attacking Windows-NT based systems increases, invariably tools will be developed by both hackers and the vulnerability testing community to exploit these type of systems. An important observation is that use of Windows-NT is not a panacea to providing network security. When configured properly, Windows-NT systems provide an effective security posture however, implementing the proper configuration is a technically challenging task.

**Allocation of Resources:**

The security posture of the OAN was obtained partly through the allocation of sufficient resources to secure this system. This is evidenced by an in-house, well-trained system administration staff section which effectively performed their jobs and associated security responsibilities. Rather than contracting out this function or using part time personnel who lack the expertise or motivation to perform this function, a work section of approximately 10 individuals perform this vital function. An extensive six month long process is used to fully train and orient newly assigned personnel to become qualified in the use of the diverse systems used in the OAN. In terms of physical facilities, the system administration function is largely performed in a single room, where all the OAN servers and gateways are located in close proximity to the system admin personnel on duty. A closely adjacent facility is used to prototype changes to the network configuration before changing the operational system. In addition, an auditing team separate from the system administrators also exists which effectively audits and monitors the OAN, as reported by the vulnerability testing team. The single auditor assigned to the OAN works closely with the system administrators, with the full time responsibility of reviewing system audit logs. This appeared to be a highly effective method of accomplishing this task since system admin personnel are usually focused on day to day activities with system fault conditions and implementing new users and capabilities.

The conclusion of this analysis was that the OAN is an effective model to demonstrate that even a system connected to the Internet can have an effective security posture. The OAN had several key factors working in its favor to achieve this rating. Obtaining this posture is not cost free or easy to accomplish. In addition to resources, it takes a strong level of commitment and management support to accomplish this feat.

## **Recommendations**

While the OAN security posture was good, it was not perfect. Several recommendations were made to improve an effective security posture. The identification and authentication procedures for remote user E-mail access could be improved by using a security token to provide a one time session key, rather than the current practice of using static passwords. While the current E-mail guard implementation is resistant to intrusion, planning for this component's replacement should continue. The implementation of a security component "firewall" or guard directly incorporating the use of security tokens for a strong level of user authentication would represent a distinct improvement over the current E-mail guard. The commendable policy of having the OAN subject to "no notice" vulnerability testing should be continued. Since even a small change in a critical parameter, such as the router rules tables can have a drastic effect on the OAN's information systems security posture, it is essential that the OAN be subject to frequent vulnerability testing. Prudent risk management dictates that any system connected to the Internet should undergo periodic evaluations since it is subject to repeated intrusion attempts. Current security policies which limit risks by strictly controlling the use of modems, fax boards and off-network access should be continued and be enforced through random audits. The emphasis and resources placed on the system administration function are a key component of the OAN's security posture and should be continued. The innovative use of a separate auditing section to monitor security related events on the system was highly effective and should also be continued.

## **Conclusion**

The increasing trend to network systems and connect these to the Internet has made securing current operational systems a high priority task. The intent of this case study is to show that it is possible to achieve an effective security posture with current technology, even on systems connected to the worldwide Internet. This type of security posture can only be achieved by allocating sufficient resources and providing the management commitment to ensure success. It is critical to note that even relatively small changes in a critical component, such as the router access control list, can have drastic effects on a system's security posture. The most effective method to determine the security posture of an operational system is to conduct periodic, in-depth vulnerability testing evaluations. The use of external intruder test teams in conjunction with the implementation of "no notice" vulnerability testing policies is a highly effective method to ascertaining the security posture of a networked system. The development and implementation of effective security policies are a critical first step to achieving a robust operational posture. Achieving an adequate security posture against both external and internal threats is a "do-able" task, and should be the objective of every networked system connected to the Internet.

## References

1. Wack and Carnahan. U.S. Department of Commerce Special Publication 800-10.  
Subject: Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,  
published by the National Institute of Standards and Technology (NIST), December 1994.
2. Cheswick and Bellovin. Firewalls and Internet Security, Addison-Wesley  
Publishing Company, 1994.
3. Mark Lottor, Subject: Internet Domain Survey January 1996. Source: <http://www.nw.com/zone/WWW/report.html>, 22 March 1996.
4. Briefing by Mr. Mike Higgins, then Chief DISA/Automated Information Systems  
Security Support Team (ASSIST), presented at the Multi Level Information Systems  
Security Initiative (MISSI) User's Conference, Orlando, Florida, October 1994.
5. Defense Information Systems Agency (DISA) document, Subject: The Electronic  
Intrusion Threat to National Security and Emergency Preparedness Telecommunications,  
published by the National Communications System (NCS), September 1993.
6. Briefing by Dr. Robert McKosky, Title: Security Technologies for the Information  
Superhighway, GTE Secure Systems Department, September 1994.